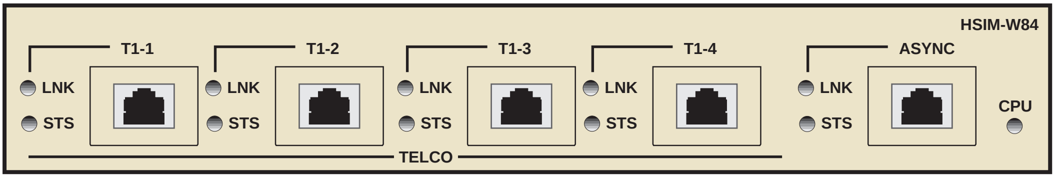
HSIM-W84
Installation Guide



9032718

Cabletron Systems

Only qualified personnel should perform installation procedures.

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© 1998 by Cabletron Systems, Inc., P.O. Box 5005, Rochester, NH 03866-5005
All Rights Reserved
Printed in the United States of America

Order Number: 9032718 July 1998

Cabletron Systems, **SmartSwitch**, **LANVIEW**, **MicroMMAC**, **QuickSET**, and **SPECTRUM** are registered trademarks, and **HSIM** is a trademark of Cabletron Systems, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

FCC Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI Notice

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Cabletron Systems, Inc. Program License Agreement

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cabletron Software Program License

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

   You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

Exclusion of Warranty and Disclaimer of Liability

1. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

   CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

United States Government Restricted Rights

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

DECLARATION OF CONFORMITY

Application of Council Directive(s): **89/336/EEC**
73/23/EEC
91/263/EEC

Manufacturer's Name: **Cabletron Systems, Inc.**

Manufacturer's Address: **35 Industrial Way**
PO Box 5005
Rochester, NH 03867

European Representative Name: **Mr. J. Solari**

European Representative Address: **Cabletron Systems Limited**
Nexus House, Newbury Business Park
London Road, Newbury
Berkshire RG13 2PZ, England

Conformance to Directive(s)/Product Standards: **EC Directive 89/336/EEC**
EC Directive 73/23/EEC
EC Directive 91/263/EEC
EN 55022
EN 50082-1
EN 60950

Equipment Type/Environment: **Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer

Mr. Ronald Fotino
Full Name

Principal Compliance Engineer
Title

Rochester, NH, USA
Location

Legal Representative in Europe

Mr. J. Solari
Full Name

Managing Director - E.M.E.A.
Title

Newbury, Berkshire, England
Location

Contents

1 Introduction

Welcome to the Cabletron Systems **HSIM-W84 Installation Guide**. This guide provides basic configuration information, hardware specifications and troubleshooting tips for the HSIM-W84. This document also provides guidelines for routing and bridging over Wide Area Networks (WANs).

Structure of this Guide

This guide is organized as follows:

Chapter 1, **Introduction**, details document conventions and provides information on getting help.

Chapter 2, **About the HSIM-W84**, describes the hardware components and software protocols and features.

Chapter 3, **Installation**, provides detailed installation instructions.

Chapter 4,**Troubleshooting**, provides detailed troubleshooting tips using the LANVIEW LEDs on the HSIM-W84.

Appendix A, **T1 Cable Specifications**, provides part number and connector information for T1 cables.

Appendix B, **Specifications and Standards Compliance**, provides hardware specifications and safety and compliance information.

Appendix C, **FCC Part 68 - User’s Information For HSIM-W84**, provides instructions required to comply with FCC Rules, Part 68.

Appendix D, **Glossary**, defines commonly used terms.

Related Documents

Use the Cabletron Systems ***QuickSTART Guide*** located in the *QuickSET* CD case to install the HSIM-W84.

Use the ***READ ME FIRST!*** document included with the HSIM-W84 to set up your computer before beginning configuration.

Use the Cabletron Systems ***CyberMONITOR User's Guide*** with the CyberMONITOR product to monitor the performance of the WAN.

Use this ***HSIM-W84 Installation Guide*** to connect your HSIM-W84 to a WAN using a Telnet connection.

Document Conventions

The following conventions are used throughout this guide:

NOTE	**Note** symbol. Calls the reader's attention to any item of information that may be of special importance.
TIP	**Tip** symbol. Conveys helpful hints concerning procedures or actions.
! CAUTION	**Caution** symbol. Contains information essential to avoid damage to the equipment.
⚡	**Electrical Hazard Warning** symbol. Warns against an action that could result in personal injury or death due to an electrical hazard.
WARNING	**Warning** symbol. Warns against an action that could result in personal injury or death.

Getting Help

If you need additional support related to this device, or if you have any questions, comments, or suggestions concerning this manual, contact the Cabletron Systems Global Call Center:

Phone	(603) 332-9400
Internet mail	support@ctron.com
FTP Login Password	ctron.com (134.141.197.25) *anonymous* *your email address*
BBS Modem setting	(603) 335-3358 8N1: 8 data bits, No parity, 1 stop bit
For additional information about Cabletron Systems or our products, visit our World Wide Web site:**http://www.cabletron.com/** For technical support, select **Service and Support**.	

Before calling the Cabletron Systems Global Call Center, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

2 About the HSIM-W84

The HSIM-W84 (Figure 2-1) is a Wide Area Network (WAN) Remote Access High Speed Interface Module (HSIM). The HSIM-W84 supports OSI Layer 2 Inverse Multiplexing (IMUX) across groups of two, three, or four T1 ports, IEEE 802.1d transparent bridging, and IP/IPX Routing. In addition, the ASYNC port connector can be used as a local console connection.

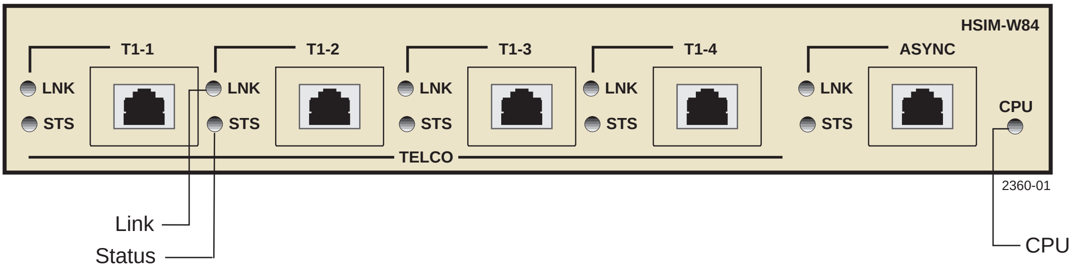


Figure 2-1 The HSIM-W84

HSIM-W84 Hardware

This section details the HSIM-W84 hardware capabilities.

WAN Connection

In Inverse Multiplexing mode, the HSIM-W84 uses a proprietary protocol based on Point-to-Point Protocol (PPP). The HSIM-W84 supports PPP, and Frame Relay protocols through the four T1 interfaces in bridging or routing mode.

- The HSIM-W84 provides four T1 interfaces through four front panel RJ45 ports. Each port includes a built-in Channel Service Unit/Digital Service Unit (CSU/DSU) for direct connections to T1 lines. The HSIM-W84 provides both Full T1 or Fractional T1 using 56 or 64 Kbps timeslots, with a total throughput of up to 1.544 Mbps per T1 interface.

Additional Features

FLASH EEPROMs — The HSIM-W84 uses FLASH Electrically Erasable Programmable Read-Only Memory (EEPROM) that allows the downloading of new and updated firmware in conjunction with Cabletron Systems *QuickSET* or any device using BootP or TFTP protocols.

LANVIEW LEDs — Cabletron Systems LANVIEW Status Monitoring and Diagnostics System is a troubleshooting tool that helps in the diagnosing of power failures, collisions, cable faults, and link problems. The LANVIEW LEDs are located on the HSIM-W84 front panel.

Remote Management Capabilities

The HSIM-W84 can be remotely managed with any SNMP network management system including the following:

- Cabletron Systems SPECTRUM for Open Systems Suite of Network Management Products
- Cabletron Systems *QuickSET*
- Third Party SNMP compliant Network Management Packages

HSIM-W84 Firmware Support

The HSIM-W84 firmware supports IEEE 802.1d bridging, and IP and IPX routing, and OSI Layer 2 Inverse Multiplexing (IMUX), which allows the four T1 channels to be used as a single, high bandwidth, WAN channel.

This device supports industry-standard protocols, security features, compression algorithms and network management tools to ensure interoperability with equipment from other vendors.

WAN Protocols

This device supports the following WAN protocols over the WAN port:

- Point-to-Point Compression Control Protocol (CCP) as defined by RFC 1962
- Point-to-Point Protocol (LCP) as defined by RFC 1661
- Point-to-Point Protocol (BNCP) as defined by RFC 1638
- Point-to-Point Protocol (IPCP) as defined by RFC 1473
- Point-to-Point Protocol (IPXCP) as defined by RFC 1552
- Frame Relay as defined by RFC 1490
- Frame Relay Data Compression Protocol (DCP) as defined by FRF.9
- Inverse Multiplexing (IMUX)
- Dynamic Host Configuration Protocol (DHCP) as defined by RFC 1541
- Network Address Translation (NAT) routing as defined by RFC 1631
- Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP as defined by RFC 1994
- Point-to-Point Protocol Link Quality Monitoring (LQM) as defined by RFC 1333
- Frame Relay Link Management Interface (LMI) as defined by ANSI T1.617 Annex D and ITU Q.933 Annex A
- Frame Relay Data Encapsulation as defined by RFC 1490
- Frame Relay Data Compression Protocol (DCP) as defined by FRF.9

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. With this protocol, options such as security, data compression, and network protocols can be negotiated over the connection.

Frame Relay is a packet-switching data communications protocol that statistically multiplexes many data conversations over a single transmission link. Data Compression (DCP) allows Frame Relay to negotiate compression over Frame Relay permanent virtual circuits (PVCs).

Inverse Multiplexing

NOTE

Cabletron Systems products that support Inverse Multiplexing (IMUX), such as the HSIM-W84, HSIM-W6, CSX400, and CSX200, must exist on both ends of the WAN link for the IMUX function to work.

Both bridging and routing functions are disabled when using the IMUX function.

Cabletron Systems Inverse Multiplexing (IMUX) feature provides enhanced throughput for users by doing each of the following:

- The IMUX function evenly distributes a data packet stream from the LAN interface through the two, three, or four Full T1 WAN interfaces on the HSIM-W84. Since the data traffic is equally shared between the interfaces, each with 1.5 Mbps throughput, the total throughput over the logical link is 3, 4.5, or 6 Mbps full-duplex. When running IMUX, the T1 interfaces that are not included in the IMUX group cannot be used.
- The IMUX function passes packet sequence information over the WAN using the Point-to-Point Protocol (PPP) to support data coherency on both ends of the link.
- Data packet streams received by the WAN interfaces on the other end of the WAN link are then recombined, ordered, and transmitted to the LAN interface.
- The IMUX function is fully configurable using *QuickSET*, which is discussed in the ***QuickSET Configuration Guide***, and the MIB Navigator command set discussed in the ***Local Management Guide for CSX400, HSIM-W6, and HSIM-W84***.

Firmware Data Compression

The STAC Electronics Stacker LZS Compression algorithm provides up to 4:1 firmware data compression for the HSIM-W84 over PPP and Frame Relay. Firmware data compression is supported in software on each T1 WAN interface for line speeds of up to 256 Kbps per interface, which is equivalent to four DS0 channels. To use data compression, compatible equipment, (such as the HSIM-W84, HSIM-W6, CSX400, and CSX200 or other vendors’ equipment which conforms to the applicable standards), must be in use at both ends of the WAN link. This firmware method of data compression is used as the default if the hardware compression module is not installed.

HDLC

Cabletron Systems has provided the High-level Data Link Control (HDLC) protocol which is used in conjunction with the Inverse Multiplexing (IMUX) feature to conserve a user's WAN bandwidth between two Cabletron Systems products, over a point-to-point connection. Cabletron Systems products such as the HSIM-W6, HSIM-W84, CSX200, and CSX400 must be in use on both ends of the WAN link for these functions to work. The HDLC (RAW) protocol reduces the amount of overhead information that needs to be contained within each data packet to direct it to its destination. This decreased packet overhead provides the IMUX functions with more bandwidth to transfer user data.

DHCP and NAT

The Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) method eliminates the expense of purchasing limited public IP addresses for each client on a local network, and the need to re-configure a client if it is moved to a different network.

The HSIM-W84 acts as a DHCP server that allows individual clients (PCs, network equipment) to take turns using a range of private IP addresses (often referred to as local IP addresses), and provides optional secondary setup features for these clients on a per-port basis. The HSIM-W84 distributes these addresses dynamically, assigning a local IP address to an individual client from a range of 253 available addresses in its table on a first-come-first-served basis. This local IP address is then "leased" for a predetermined amount of time, which is configured for the particular port. The HSIM interface provides DHCP services for one Class C subnet and secondary setup features for individual clients support the use of a default gateway, domain name and WINs server.

On the Wide Area Network (WAN) side, the Network Address Translation (NAT) routing method is used to enable clients assigned with local IP addresses to use the public IP address(es) of the HSIM-W84 WAN interface(s) to access the WAN.

NOTE

A private or "local" network is referred to as a sub network that is using private or "local" IP addresses. An "outside" network refers to a Wide Area Network (WAN) commonly known as an Internet where registered public IP addresses are required.

The NAT method **(that is supported only on interface T1-1)** allows several DHCP clients on a sub network to connect to WAN clients by allowing the DHCP clients to share a single public IP address. When the HSIM-W84 uses NAT, the NAT method modifies the IP headers and addresses, and the selected fields in upper layer protocol headers. This is done to replace the hidden local IP addresses from the sub network with one or more public InterNic assigned IP addresses that can be sent over the outside network on the HSIM-W84 T1-1 WAN interface. Once the HSIM-W84 is assigned at least one public IP address, over 250 IP clients can share this address simultaneously using NAT. This public IP address is assigned statically by the Internet Service Provider (ISP), or equipment installer.

Point-to-Point Protocol

PPP is a data link layer industry standard WAN protocol for transferring multi-protocol data traffic over point-to-point connections. It is suitable for both high-speed synchronous ports as well as lower speed asynchronous dial-up ports. With this protocol, options such as security and network protocols can be negotiated over the connection.

The STAC Electronics Stacker LZS Compression Protocol is supported over PPP providing up to 4:1 data compression.

Frame Relay Protocol

Frame Relay can be defined as a “packet mode” service, organizing data into individually addressed units known as “frames”. Frame Relay eliminates all Layer 3 processing. Only a few Layer 2 functions are used, such as checking for a valid, error free frame, but not requesting retransmission if an error is found. Frame Relay uses a variable length framing structure, which, depending on user data, can range from a few to more than a thousand characters.

A Frame Relay Network will often be depicted as a cloud, because the Frame Relay Network is not a single physical connection between one endpoint and another. Frame Relay protocol is based on the concept of Virtual Circuits (VCs). VCs are two-way, software defined data paths between two ports that take the place of private lines in the network. There are two types of Frame Relay connections; Switched Virtual Circuits (SVCs), and Permanent Virtual Circuits (PVCs).

Permanent Virtual Circuits, or PVCs, are set up via a network management system, and initially defined as a connection between two sites, or endpoints. PVCs may be added as the demand arises for more bandwidth, alternate routing, or more sites. PVCs are fixed paths, not available on demand, or on a call-by-call basis. Although the actual path through the network may change from time to time, such as when automatic rerouting takes place, the beginning and end of the circuit will not change.

Switched Virtual Circuits, or SVCs, are available on a call-by-call basis using the SVC signaling protocol (Q.933). The network must quickly establish the connection, and allocate bandwidth based on the user's request.

In a Frame Relay frame, user data packets are not changed in any way. A two byte header is appended to the frame. Contained in this header is a 10-bit number called the Data Link Connection Identifier (DLCI). The DLCI is the "virtual circuit" number which corresponds to a particular destination. The DLCI allows data coming into a Frame Relay switch to be sent across the network using a three-step process: Check the integrity of the frame and discard it if it is in error, look up the DLCI in a table and if not intended for this link, discard the frame. If the frame passes the previous tests, relay the frame toward its destination out the specific port specified in the table.

The ANSI standard defines a mechanism for the network to signal the existence of congestion, called Explicit Congestion Notification (ECN) bits. Frame Relay uses FECN (Forward ECN) and BECN (Backward ECN) bits to notify end user devices about network congestion. Although the Frame Relay protocol does not respond to congestion, some higher layer protocols for end user devices may respond to ECNs by recognizing that delays have increased, or that frames have been dropped.

The IP-OSPF Routing Protocol

Open Shortest Path First (OSPF) is a link state routing protocol developed for Internet Protocol (IP) networks. OSPF distributes routing information between routers belonging to a single autonomous system. In an autonomous system, routers exchange routing information through a common routing protocol.

OSPF was designed primarily for the Internet environment and supports variable length subnet masks, Type of Service (TOS) based routing, packet authentication, and the tagging of externally derived routing information.

OSPF, based upon link-state technology, was developed by the Internet Engineering Task Force (IETF). The IETF developed OSPF based upon the shortest path first algorithm to serve large, heterogeneous networks.

A key feature of OSPF is the speed in which it responds to topological changes, commonly referred to as "convergence time." OSPF generates a minimal amount of routing protocol traffic compared to most distance vector protocols.

Cabletron's implementation of OSPF is based on RFC 1247 — OSPF Version 2 and RFC 1253 — OSPF Version 2 Management Information Base.

IP-OSPF Hierarchy

IP-OSPF operates within a hierarchy of entities:

Autonomous System

An Autonomous System (AS) is a set of routers and networks under a common administration. Routers inside an AS are called “interior gateways” and the protocol is called Interior Gateway Protocol (IGP). OSPF is an IGP.

Every OSPF routing domain must have a backbone. An OSPF backbone distributes routing information between areas in an OSPF routing domain. The backbone of an OSPF routing domain system is an OSPF area possessing an area id of 0.0.0.0.

Areas

Areas are groups of networks and attached hosts. A router’s topology database includes area links, and summarized and external links depicting the autonomous system topology. From this database, routers calculate a route using the shortest-path tree algorithm.

The Hello Protocol

The Hello Protocol establishes and maintains neighbor relationships, and ensures bidirectional communications among neighboring routers. Hello packets are sent out all router ports periodically. A designated router is chosen by the Hello Protocol on multi-access networks and controls adjacencies formed over the network.

Neighbors and Adjacency

The OSPF routing protocol establishes adjacencies among neighboring routers which facilitate the exchange of routing information. Neighboring routers have interfaces to a common network and are discovered by OSPF’s Hello Protocol.

Area Border Router

Area Border Routers (ABR) connect networks together. These routers have multiple interfaces and participate in multiple areas. There must be at least one area border router in each area connecting that area to a backbone. An ABR maintains a separate link-state database per area to which it is attached.

Designated Router

Designated Routers (DR) are used by OSPF to reduce adjacencies. Other routers establish adjacencies and synchronize databases only with the designated router and backup designated router. These routers perform two key functions for the OSPF routing protocol:

- The designated router creates a network links advertisement which lists the set of routers, including the designated router, attached to the network.
- The designated router is adjacent to all routers on the network and plays a central role in the synchronization of link-state databases across adjacencies.

One DR is elected for each network and is elected by using the Hello Protocol.

If one or more routers have declared to be the DR in their Hello packets, the one with the highest Router Priority becomes the DR. If more than one router has identical router priority, then the router with the highest router ID becomes DR.

Backup Designated Router

Backup Designated Routers (BDR) are used for each multi-access network. The BDR is adjacent to all routers on the network and becomes the Designated Router if the existing Designated Router fails. The BDR does not generate network link advertisements and is also elected by the Hello Protocol.

The Backup Designated Router is chosen from those routers who have not declared themselves to be the Designated Router. If a one or more routers have declared itself to be the BDR in their Hello packets, the one with the highest Router Priority becomes the BDR. If no routers have declared themselves to be BDR, then the router with the highest router ID becomes BDR.

Detailed information on the OSPF protocol is documented in RFC 2178.

PAP and CHAP Security

The HSIM-W84 supports the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) under PPP.

PAP provides verification of passwords between devices using a 2-way handshake. One device (peer) sends the system name and password to the other device (authenticator). Then the authenticator checks the peer’s password against the configured remote peer’s password and returns acknowledgment.

CHAP is more secure than PAP as unencrypted passwords are not sent across the network. CHAP uses a 3-way handshake and supports full or half-duplex operation.

In half-duplex operation, the authenticator device challenges the peer device by generating a CHAP challenge, and the challenge contains an MD5 algorithm with a random number that has your encrypted password and system name. The peer device then applies a one-way hash algorithm to the random number and returns this encrypted information along with the system name in the CHAP response. The authenticator then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends locally.

Full-duplex operation places an additional step to the half-duplex operation that mirrors the operation discussed above for a peer to validate the authenticator. The peer device challenges the authenticator by generating a CHAP challenge, and the authenticator returns a CHAP response.

The peer device challenges the authenticator device by generating a CHAP challenge, and the challenge contains an MD5 algorithm with a random number that has your encrypted password and system name. The authenticator device then applies a one-way hash algorithm to the random number and returns this encrypted information along with the system name in the CHAP response. The peer device then runs the same algorithm and compares the result with the expected value. This authentication method depends upon a password or secret, known only to both ends locally.

LQM

Link Quality Monitoring (LQM) is a link control mechanism used with PPP to determine when and how often a link is dropping data in units of packets and octets. Link Quality Monitoring accomplishes this by providing Link-Quality-Reports to determine if the quality of the link is adequate for operation. Link Quality Monitoring provides separate measurements for both incoming and outgoing packets that are communicated to both ends of the link. The PPP LQM mechanism carefully defines the Link-Quality-Report packet formats, and specifies reference points for all data transmission and reception measurements. The LQM implementation maintains successfully received packet and octet counts, and periodically transmits this information to its peer using Link-Quality-Report packets.

Bridging and Routing

Bridging — Bridging connects two or more separate networks together. The bridge examines a portion of each network frame called the header. This header contains control information for the frame. The bridge compares the destination address of the frame to a table of source addresses (bridges dynamically learn the physical location of devices by logging the source addresses of each frame and the bridge port the frame was received on in the source address table). In transparent bridging, the decision to forward the frame is based on this comparison. If the address indicates that the sending station and the destination station are on the same side of the bridge, the frame is not forwarded across the bridge. If the addresses do not indicate that, the bridge forwards the broadcast frame across the bridge to the other network(s).

Bridging allows frames to be sent to all destinations regardless of the network protocols used. It also allows protocols that cannot be routed (such as NETBIOS) to be forwarded, and optimizes internetwork capacity by localizing traffic on LAN segments. A bridge extends the physical reach of networks beyond the limits of each LAN segment. Filters can be used to increase network security in bridged networks, and restrict message forwarding by using user-built address tables (non-transparent bridging).

Routing — Routing provides a way to transfer user data from source to destination over different LAN and WAN links using one or more network protocol formats. Routing relies on routing address tables to determine the best path for each packet. Routing tables can be seeded (i.e., addresses for remote destinations are placed in the table along with network address masks and a metric for path latency). Routing tables are also built dynamically (i.e., the location of remote stations, hosts and networks are updated through inter-router protocols). Routing helps to increase network capacity by localizing traffic on LAN segments and broadcasts that would result from bridged traffic. It also provides security by isolating traffic on segmented LANs. Routing extends the world-wide reach of networks.

HSIM-W84 Bridging and Routing — The HSIM-W84 can operate as a bridge, a router, or both. The HSIM-W84 operates as a router for network protocols that are supported when routing is enabled and operates as a bridge when bridging is enabled. When both bridging and routing are enabled, routing takes precedence over bridging (i.e., the HSIM-W84 uses the protocol address information of the packet to route the packet to the correct destination, and if the protocol is not supported, the device uses the MAC address information to bridge the packet).

Operation of the HSIM-W84 is influenced by routing and bridging controls and filters set during HSIM-W84 configuration. General IP routing, and routing or bridging from specific remote routers are controls set during the configuration process.

IEEE 802.1d Bridging — The HSIM-W84 supports the IEEE 802.1d standard for LAN to LAN bridging. This bridging algorithm learns the low-level MAC addresses of each LAN constituent and uses this information to decide whether to transmit the packet to another LAN via a WAN connection, or keep it local. Part of the bridging standard used, called Spanning Tree Protocol, supports multiple, redundant paths for LAN to LAN bridging, yet prevents data loops and duplication. This adds fault tolerance to a system of LANs, since, if one WAN data path fails, another may be substituted automatically.

IP Routing — IP routing support provides the ability to process TCP/IP frames at the network layer for routing. IP routing support includes the Routing Information Protocol (RIP) that allows the exchange of routing information on a TCP/IP network. The HSIM-W84 receives and broadcasts RIP messages to adjacent routers and workstations.

IPX Routing — Internet Packet Exchange (IPX) routing support provides the ability to process Novell proprietary frames at the network layer for routing. IPX routing support includes the Routing Information Protocol (RIP) that allows the exchange of routing information on a Novell NetWare network.

Bridging and Routing Protocol Filtering

Filtering is used to allow efficient usage of network resources and provide security for your network and hosts.

IP Internet Firewall — The HSIM-W84 supports IP Internet Firewall filtering to prevent unauthorized access to your system and network resources from the Internet or a corporate Intranet. Security can be configured to permit or deny IP traffic. The security is established by configuring IP access filters, which are based on source IP address, source mask, destination IP address, destination mask, protocol type, and application port identifiers for both the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). These IP access filters allow individual IP source and destination pair filtering as well as IP address ranges and wild carding to match any IP address. These Firewall filters can be defined to allow inbound only, outbound only, or bi-directional IP communication up to the UDP and TCP application port level. Firewall access filters provide a lot of flexibility to establish a powerful IP security barrier.

The HSIM-W84 supports the IP Access Control (from the ctip-mib) Internet Firewall Filter.

Bridge Filtering — Bridge filtering allows a network administrator to control the flow of packets across the HSIM-W84. Bridge filtering can be used to “deny” or “allow” packets based on a “matched pattern” using a specified position and hexadecimal content within the packet. This enables restricting or forwarding of messages based on address, protocol, or data content.

Common uses include preventing access to remote networks, controlling unauthorized access to the local network, and limiting unnecessary traffic.

The HSIM-W84 supports the following Bridge Filters:

- dot1d.Static Filters (IETF RFC 1493)
- Ethernet Special Filtering Database (from the ctbridge-mib)

System Passwords

System passwords allow you to control access to the HSIM-W84 by establishing three passwords. Each password provides varying levels of access to the HSIM-W84. The default password for each access level is preset to *public*.

The following definitions explain each of the three levels of access:

read-only — This access level allows reading of device parameters not including system passwords.

read-write — This access level allows editing of some device configuration parameters not including changing system passwords.

super-user — This access level allows full management privileges, allowing you access to *QuickSET*.

Simple Network Management Protocol (SNMP)

The HSIM-W84 provides SNMP agent support for the following: standard and Enterprise Specific Management Information Bases (MIBs), and support for standard and Enterprise Specific SNMP Traps. SNMP is also used internally for configuration of the HSIM-W84. The active SNMP agent within the HSIM-W84 accepts SNMP requests for status, statistics and configuration updates. Communication with the SNMP agent occurs over the LAN or WAN connection. Any management application using SNMP over UDP/IP has access to the local SNMP agent.

SNMP MIB Support

SNMP MIBs are databases of objects used for managing and determining the status and configuration of an SNMP compliant device.

The following SNMP MIBs are supported by the HSIM-W84:

- MIB II RFC 1213
- RMON MIB RFC 1271

- DS1 and E1 MIB RFC 1406 (Digital Signal Level 1 [T1/E1 interface types])
- IETF Bridge MIB RFC 1493
- IP Forwarding MIB RFC 1354
- PPP LCP MIB RFC 1471 (Point-to-Point Protocol, Link Control Protocol)
- PPP IPCP MIB RFC 1473 (IP Control Protocol)
- PPP BNCP MIB RFC 1474 (Bridge Network Control Protocol)
- IPXCP MIB RFC 1552 (PPP Internetworking Packet Exchange Control Protocol)
- Frame Relay DTE MIB RFC 1315
- Security MIB RFC 1472 (CCP, PAP, and CHAP)
- RS-232 MIB RFC 1317
- LQM MIB RFC 1989
- PPP MP RFC 1990
- Frame Relay MultiProtocol Encapsulation MIB RFC1490
- OSPF V2 RFC2178
- OSPF V2 MIB RFC1850

Cabletron Enterprise MIBs

Cabletron Enterprise MIBs include the following: CTWAN-MIB, CTMIB2-EXT-MIB, CTDOWNLOAD-MIB, CTBRIDGE-MIB, RREV-4-MIB, CTROUTER-MIB, CTFAULT-MIB, CTIP-MIB, CHASSIS-MIB, CTNETDIAG-MIB, IP-MIB, IPX-MIB, CTDEFAULT-MIB, CTNAT-MIB.TXT, CTDHCP-MIB.TXT, and CTWAN-IMUX-MIB.

SNMP Trap Support

SNMP Traps are notifications of network events sent by an SNMP compliant device to an SNMP management station.

The following SNMP Traps are supported by the HSIM-W84:

- IETF Standard Traps:
  - Warm Start Trap Type Code #1 RFC 1214
  - Bridge New Root Trap Type Code #1 RFC 1493
  - Bridge Topology Change Trap Type Code #2 RFC 1493

- Cabletron Enterprise Traps:
  - Port Segmented Trap Type Code #257(0x101)rrev4-mib
  - Port Operational Trap Type Code #258(0x102)rrev4-mib
  - Port Link Up Trap Type Code #259(0x103) rrev4-mib
  - Port Link Down Trap Type Code #260(0x106) rrev4-mib
  - Environmental Temperature Hot Trap Type Code #282(0x11A) brrev4-mib
  - Environmental Temperature Normal Trap Type Code #284(0x11C) rrev4-mib
  - IP Event Log Change Trap Type Code #1280(0x500) ctip-mib

    The following is a list of IP Events that are logged and that create the IP Event Log Change Trap.

    - IP Routing has been disabled on interface #
    - IP Routing has been enabled on interface #
    - IP Forwarding has been enabled on interface #
    - IP MTU size has been changed on interface #
    - IP Framing Type has been changed on interface #
    - IP has detected Link UP on interface #
    - IP has detected Link DOWN on interface #
    - IP Primary address has been changed on interface #
    - IP Secondary address has been changed on interface #
    - IP Access Control Lists have been enabled on interface #
    - IP Access Control Lists have been disabled on interface #
    - IP has detected Port UP (WAN devices only)
    - IP has detected Port DOWN (WAN devices only)
    - IP Proxy ARP has been disabled on interface #
    - IP Proxy ARP has been enabled on interface #
    - IP RIP has been enabled on interface #
    - IP RIP has been disabled on interface #
  - IPX Event Log Change TrapType Code #1281(0x501)ctipx-mib

    The following is a list of IPX Events that are logged and that create the IPX Event Log Change Trap.

    - IPX Routing has been disabled on interface #
    - IPX Routing has been enabled on interface #
    - IPX Forwarding has been enabled on interface #

- IPX MTU size has been changed on interface #
- IPX Framing Type has been changed on interface #
- IPX has detected Link UP on interface #
- IPX has detected Link DOWN on interface #
- IPX Primary address has been changed on interface #
- IPX Access Control Lists have been enabled on interface #
- IPX Access Control Lists have been disabled on interface #
- IPX has detected Port UP (WAN devices only)
- IPX has detected Port DOWN (WAN devices only)
- IPX RIP has been enabled on interface #
- IPX RIP has been disabled on interface #
- IPX SAP has been enabled on interface #
- IPX SAP has been disabled on interface #

Software and Firmware Upgrades

Software and Firmware upgrades can be performed remotely through the Windows-based QuickSET utility application. Refer to the ***QuickSET Configuration Guide*** for instructions. QuickSET allows you to retrieve or upgrade the firmware, software, and configuration files from its **Firmware Upgrade** menu by selecting the TFTP/BootP Services Window to access a TFTP (Trivial File Transfer Protocol) server.

3 Installation

This chapter outlines the procedure for attaching the HSIM-W84 to the network. To install the HSIM-W84 you need the following items:

- Antistatic wrist strap (provided with the HSIM-W84)
- Phillips screwdriver

Only qualified personnel should perform installation procedures.

Unpacking the HSIM-W84

Unpack the HSIM-W84 as follows:

1. Remove the shipping material covering the HSIM-W84 in the shipping box.
2. Carefully remove the HSIM-W84 from the shipping box. Leave the module in its non-conductive bag until you are ready to install it.
3. Attach the antistatic wrist strap (refer to the instructions on the antistatic wrist strap package).
4. After removing the module from its non-conductive bag, visually inspect the device. If there are any signs of damage, contact Cabletron Systems (refer to **Chapter 1**, **Getting Help**) immediately.

Guidelines for Installations

Only qualified personnel should perform installation procedures.

Installation sites must be within reach of the network cabling and meet the requirements listed below:

- A properly grounded power receptacle must be within seven feet of the location.

- In a shelf installation, the shelf must be able to support 13.6 kg (30 lb) of static weight for each device on the shelf.
- Maintain a temperature of between 5°C (41°F) and 40°C (104°F) at the installation site with fluctuations of less than 10°C (50°F) per hour.
- Maintain a two-inch clearance for each side and the back of the device for adequate ventilation.

Installing an HSIM

You can install an HSIM-W84 in any Cabletron Systems device that supports HSIM technology (e.g., SmartSwitch 2200, SmartSwitch 6000). Refer to the release notes for the version of firmware running on the Cabletron Systems device to ensure that the HSIM-W84 is supported. The following sections provide generic instructions for installing an HSIM-W84 in a SmartSwitch interface module, or SmartSwitch standalone device. Refer to your specific interface module, or standalone device documentation for exact HSIM slot and connector locations.

CAUTION

The HSIM-W84 and the host module or standalone device are sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could result in damage to the HSIM-W84, the host module or standalone device.

Installing an HSIM in a SmartSwitch 6000 Interface Module

To install an HSIM in a module that supports HSIM technology refer to **Figure 3-1** and **Figure 3-2** and complete the following steps:

1. Disconnect all network cables from the interface module. Note the ports to which these cables are attached.
2. Attach the disposable antistatic wrist strap.
3. Unlock the top and bottom plastic locking tabs of the module faceplate.
4. Slide out the interface module and place it on its side with the internal components facing up.
5. Remove and save the two faceplate mounting screws securing the HSIM coverplate and remove the coverplate. See **Figure 3-1**.
6. Remove and save the two standoff screws.

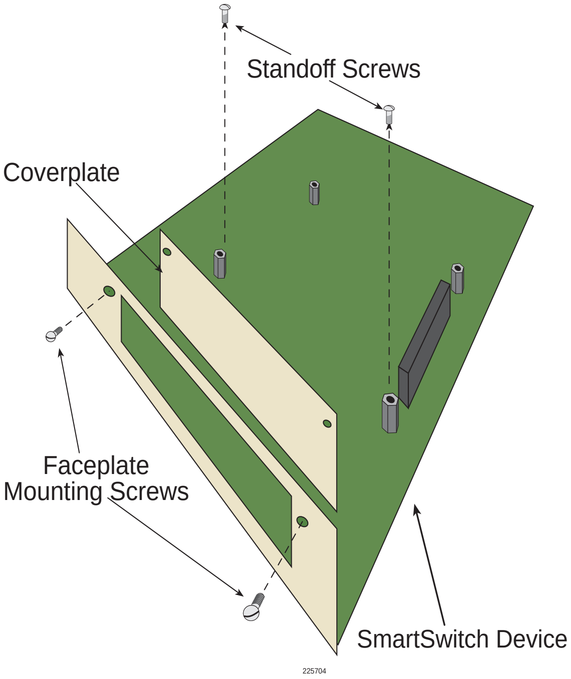


Figure 3-1 Removing the HSIM Coverplate

7. Place the HSIM behind the module faceplate. See Figure 3-2.
8. Ensure that the standoffs on the interface module align with the standoff screw holes on the HSIM to prevent bending pins. Then insert the connector pins of the HSIM into the HSIM connector on the interface module.
9. Press down firmly on the back of the HSIM until the pins slide all the way into the connector holes.
10. Secure the HSIM to the faceplate using the two screws saved in step 5.
11. Secure the HSIM to the standoffs with the screws saved in step 6.
12. Reinstall the interface module into the SmartSwitch 6000 chassis.
13. Reattach the network cabling to the module.

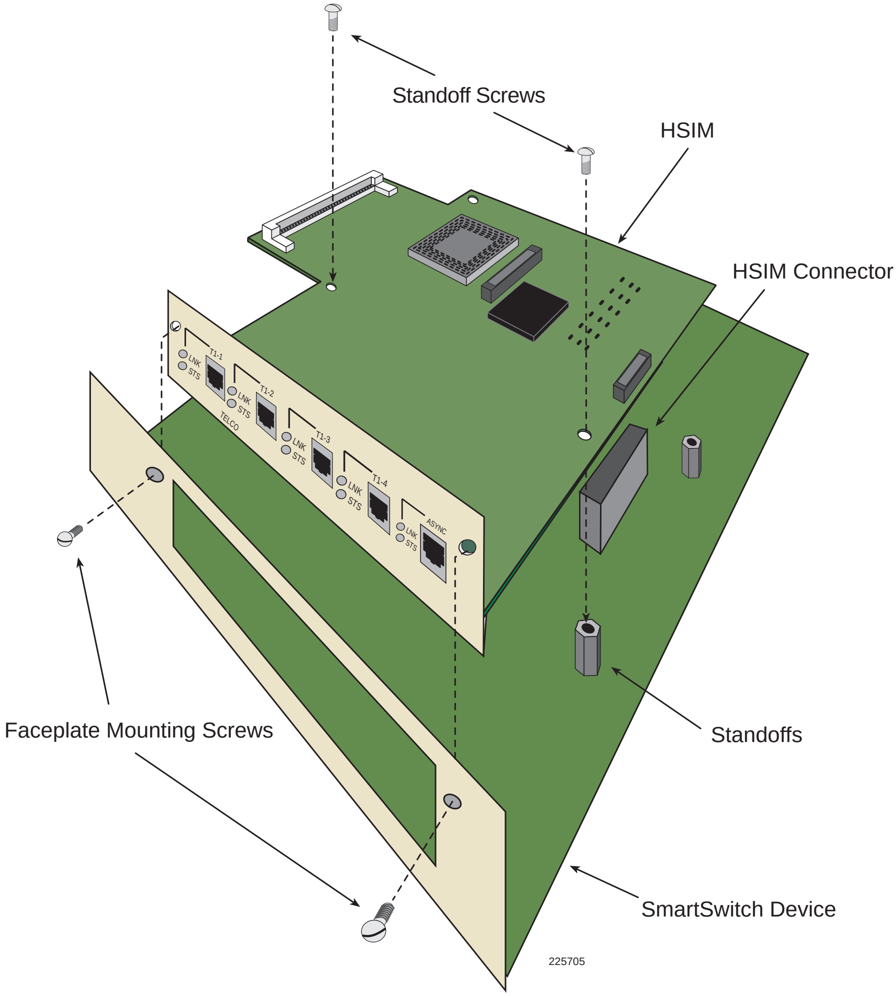


Figure 3-2 Installing the HSIM

Installing an HSIM in a SmartSwitch Standalone Device

To install an HSIM into a SmartSwitch standalone device that supports HSIM technology refer to **Figure 3-1** and **Figure 3-2**, and perform the following steps:

1. Power down the standalone device and remove the power cord.
2. Disconnect all network cables from the standalone device. Note the ports to which these cables attach.

Ensure that you remove the power cord and ONLY the screws required to remove the standalone device cover. Failure to comply could result in an electric shock hazard.

3. Attach the antistatic wrist strap.
4. Remove the standalone device cover (refer to your specific standalone device documentation for instructions on removing the standalone device cover).
5. Remove and save the two faceplate mounting screws securing the HSIM coverplate and remove the coverplate. See **Figure 3-1**.
6. Remove and save the two standoff screws. See **Figure 3-1**.
7. Place the HSIM behind the standalone device faceplate. See **Figure 3-2**.
8. Ensure that the standoffs on the standalone device align with the standoff screw holes on the HSIM to prevent bending the pins and insert the connector pins of the HSIM into the HSIM connector on the standalone device motherboard.
9. Press down firmly on the back of the HSIM until the pins slide all the way into the connector holes.
10. Secure the HSIM to the faceplate using the screws saved in step 5.
11. Secure the HSIM to the standoffs using the screws saved in step 6.

Ensure that the standalone device cover is in place before reconnecting the power cord.

12. Reattach the standalone device’s cover to the standalone device and reconnect the power cord.
13. Reconnect the standalone device to your network.

CSX-COMP/ENCR Installation

This section contains instructions on how to install the COMP/ENCR into the HSIM-W84. To help eliminate any potential problems during or after installation, read and understand the following steps:

1. Attach one end of the antistatic wrist strap to your wrist and the other end to an approved electrical ground.
2. Unpack the CSX-COMP/ENCR by carefully removing it from the shipping box and then from the protective plastic bag. Do not cut the bag as the device could be damaged. If there are any signs of damage, contact the Cabletron Systems Global Call Center (refer to **Chapter 1**, **Installation**).
3. Install the CSX-COMP/ENCR in the HSIM-W84 by unlocking the top and bottom plastic locking tabs of the module faceplate. Slide out the module and place it on its side with the internal components facing up.

NOTE

Ensure that the CSX-COMP/ENCR is aligned such that its connector pins correctly align with the D-Type connector on the HSIM-W84.

4. Locate the D-Type connector and the standoffs on the HSIM-W84 (refer to **Figure 3-3**).
5. The D-Type connector pins of the CSX-COMP/ENCR only fits one way onto the HSIM-W84 D-Type connector. Lower the CSX-COMP/ENCR onto the standoffs and align the connector with the connector pins. Carefully insert the connector pins of the CSX-COMP/ENCR into the connector on the HSIM-W84.
6. Press down firmly on the CSX-COMP/ENCR until the pins fit all the way into the connector.
7. Secure the CSX-COMP/ENCR with the standoff screws supplied with the CSX-COMP/ENCR.

The CSX-COMP/ENCR installation is complete.

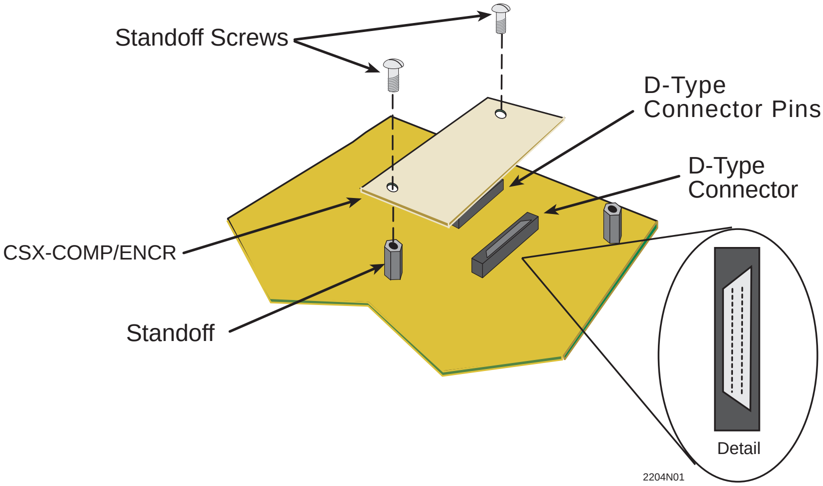


Figure 3-3 CSX-COMP/ENCR

4 Troubleshooting

Use this chapter in conjunction with the LANVIEW status monitoring and diagnostic LEDs on the HSIM-W84 to diagnose power failures, cable faults and link problems. Figure 4-1 shows the front panel LEDs. Table 4-1 through Table 4-5 describe the LED states of the HSIM-W84.

If you are having difficulty installing and configuring the HSIM-W84, perform the following steps:

- Review the ***HSIM-W84 QuickSTART Guide*** to insure proper installation.
- Check that all cables and connectors have been attached properly.
- Verify that power has been applied to the HSIM-W84.

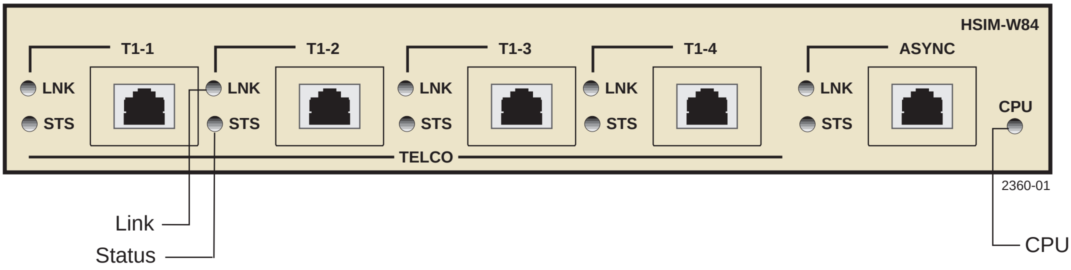


Figure 4-1 HSIM-W84 Front Panel LEDs

Table 4-1 HSIM-W84 Hardware LED States

LED	Color	State
Processor (CPU)	OFF	Power Off
	RED	Fault condition detected
	AMBER	Testing in progress
	GREEN	Functional

Table 4-2 HSIM-W84 ASYNC LED States (Console Connection Only)

LED	Color	State
Status (STS)	AMBER	Console connection; Data Carrier Detect (DCD); No Data Set Ready (DSR)
	AMBER (blinking)	Test mode
	GREEN	Modem with connection; DCD; DSR
	GREEN (blinking)	Modem, no connection; DSR; No DCD
Link (LNK)	RED	Modem connection; Request To Send (RTS); No Clear To Send (CTS)
	AMBER (blinking)	Traffic; Modem or console connection
	GREEN	Modem connection; RTS; CTS asserted

Table 4-3 shows the console connection to the ASYNC port. The configuration setup for a VT100 Mode Terminal is 8 bits, No parity, 1 stop bit, and 9600 baud.

Table 4-3 HSIM-W84 ASYNC Console Connection Pinout

PIN	Description
1	VT Receive Data
2	VT Data Terminal Ready (DTR)
4	VT Transmit Data
5	Ground

Table 4-4 HSIM-W84 WAN Link (LNK) LED States

LED	Color	State
Link (LNK)	OFF	WAN interface not configured
	RED	No Link/Connection (Fault) on the WAN interface
	AMBER	Transmit (TX) and/or receive (RX) traffic
	GREEN	Link and port is active
	GREEN (blinking)	Link and port is in standby

Table 4-5 HSIM-W84 WAN Status (STS) LED States for T1 Ports

LED	Color	State
Status (STS)	OFF	Normal or disabled
	RED	Red Alarm
	AMBER	Yellow alarm
	AMBER (blinking)	Port in test mode

Troubleshooting HSIM-W84 Hardware

The following sections describe the LED states for the hardware, ASYNC console connection, and WAN connection, and show how to troubleshoot the HSIM-W84 based on these LED states.

SmartSwitch Standalone or Module Power (PWR) LED is OFF — Check that the power connection is firmly attached to the back panel of the SmartSwitch Standalone or Module, and the other end to an active power source.

Processor (CPU) LED is OFF — If the CPU stays OFF for an extended amount of time, and the power (PWR) light remains on, the CPU is in an unknown state. Contact Cabletron Systems Global Call Center for technical support (refer to **Getting Help** in **Chapter 1**).

Processor (CPU) LED is RED — Processor has detected a fault condition. Contact Cabletron Systems Technical Support (refer to **Getting Help** in **Chapter 1**).

ASYNC Console Connection

Link (LNK) LED is OFF — There is normal console operation and no traffic on the interface.

Link (LNK) LED is RED or GREEN — The ASYNC port is connected for modem operation. Check the cabling and console connection pinout.

Link (LNK) LED is AMBER — There is traffic on the interface.

Status (STS) LED is OFF — The ASYNC port is disconnected or Data Carrier Detect (DCD) and Data Set Ready (DSR) are inactive.

Status (STS) LED is AMBER — The console connection is detected. The Data Carrier Detect (DCD) is active, while the Data Set Ready (DSR) is inactive. If the port does not function, check the cabling, console connection pinout, and VT configuration.

Status (STS) LED is GREEN or GREEN (Blinking) — The ASYNC port is connected for modem operation. Data Set Ready (DSR) is Active. Check the cabling and console connection pinout.

Status (STS) LED is AMBER (Blinking) — The HSIM-W84 is in test mode.

- The HSIM-W84 is running its Power-up Diagnostic Tests.
- Loopback Testing is underway on the ASYNC interface.

Troubleshooting the WAN

Link (LNK) LED is OFF — The WAN interface is not configured for operation. Use QuickSET or Local Management to make sure that the WAN interface is configured correctly.

Link (LNK) LED is RED — The WAN interface is configured, but there is no signal indicating that a valid connection is present on the WAN interface.

- Check that the HSIM-W84 and the device at the other end of the segment are powered up.
- Use QuickSET or Local Management to make sure that both WAN interfaces, local and remote, are configured correctly.
- Check to ensure that the correct cable is being used.
- Check to ensure that the cable has continuity and is fully installed.
- Check with the WAN Service Provider to ensure that the circuit has been configured by them and is active.

Link (LNK) LED is GREEN (blinking) — The port has a good link, and is in Standby mode.

- Check with the Network Administrator to see if management placed the port in Standby mode.
- Ensure that the protocol that you want to run has been properly selected at both ends and the time slots have been allocated if applicable.

Status (STS) LED is OFF — The port is operating normally. If it is not, and this LED is OFF the port may be disabled. Use QuickSET or Local Management to make sure that the WAN interface on the Local device is configured correctly.

Status (STS) LED is RED — A RED alarm indicates that the WAN connection is not receiving proper framing or has lost framing from the HSIM-W84.

- Verify the use of proper cabling on the WAN connection.
- Check Frame Type selection on the WAN Physical Configuration and line coding.
- Possible bad cabling between Telco and HSIM-W84.

Status (STS) LED is AMBER — The device is in Yellow alarm mode. A Yellow alarm indicates that the HSIM-W84 is

receiving proper framing from the Telco, but the Telco is not receiving proper framing.

- Check for faulty or incorrect cabling between Telco and HSIM-W84.
- Request that the Telco verify the configuration and operation of the circuit.

Status (STS) LED is AMBER (blinking) — Device is in test mode.

- The HSIM-W84 is running its Power-up Diagnostic Tests.
- Loopback Testing is underway on a WAN circuit. Loopback testing can be initiated by the Telco.

Investigating Software Configuration Problems

Software problems usually occur when your software configuration contains incomplete or incorrect information.

Connection to Device Fails During Software Configuration

- For a LAN connection, verify that the IP address matches the IP address previously stored into the configuration of the router. You must have previously (through *QuickSET*) set the Ethernet LAN IP address and Subnet Mask, enabled IP routing, saved the Ethernet configuration changes and rebooted the router for the new IP address to take effect.
- Check that your LAN cable is wired correctly and each end securely plugged in.
- Make sure that an IP route exists between your local PC and the HSIM-W84. The PC and HSIM-W84 must be on the same IP subnetwork or the HSIM-W84 must be reachable through a router on your LAN.
- Check Network TCP/IP properties under Windows 95 or Windows NT, as described in the ***Read Me First!*** document.

User Cannot Communicate with Remote Network Station

If Bridging,

- Check that the Bridging Default Destination is set.
- Check that bridging to/from the remote router is set on.
- Be sure to reboot if you have made any bridging destination or control changes.

If TCP/IP Routing,

- Check that TCP/IP Routing is set on and is enabled at the remote end.
- Check that the IP address of the LAN beyond the remote router is correct, as well as the associated Subnet Mask.
- If the remote router WAN IP address and Subnet Mask are required, check that they have been specified correctly.
- Check that, if required, the source and remote WAN IP addresses are on the subnetwork.
- Check that you have seeded the routing table, if RIP is not allowed to flow on the WAN link.
- Be sure to reboot if you have made any IP address, control or protocol option changes.

Troubleshooting the Frame Relay Connection

There are three troubleshooting tools available. The first has always been available and is LM. The second is the FR Error MIB Table, and reflects LMI or DLCI data errors. The third is new and is available as the Mib Nav command: “fr”.

Communication with the FR switch is done through one of two methods:

Asynchronous Status Messages — At any time the Fr Switch can send an unsolicited (no polling from us) message to us. Each message contains information on one DLCI and one only. It has the DLCI number and the DLCI state. We don’t respond to this message, but we do adjust what we know about DLCIs based on this information.

Synchronous Polling Messages — The t391 timer for the ANSI/ITU Frame Relay forms the basis for polling between the FR switch and the FR DTE (us). We transmit a STATUS ENQUIRY every t391 seconds (10 by default) to the FR switch. We expect a STATUS RESPONSE, which contains information on the DLCIs the switch has assigned to us. Every other t391 cycle we sent out a LINK INTEGRITY VERIFICATION ENQUIRYmessage (LIV). We expect to get a LINK INTEGRITY VERIFICATION RESPONSE back from the Fr switch before out t391 polling cycle expires. This is a keep alive message that does no more than let us know the link between us and the FR switch is still alive.

The information provided in a FULL STATUS RESPONSE, or ASYNCHRONOUS STATUS MESSAGE basically has two parts, the FR Switch provides a DLCI number, and whether that DLCI is in the Active or Inactive state.

Active State — means that both ends of the connection (this DTE and the DTE at the other end of the WAN cloud) are speaking correctly to the FR DCE Switches in the WAN cloud. The Inactive state means that either the local or far end DTE is either just starting up and has not completed its initial negotiation with the FR Switch, or there is some sort of LMI error. Data (other than LMI negotiation messages) will only be transferred when in the Active state.

Invalid — the third state value is reported locally only. It is not done by polling the FR switch. This is done if the physical connection has some sort of problem. The circuit will remain in the Invalid state until negotiation with the FR DCE Switch completes successfully.

A T1 Cable Specifications

NOTE

For T1 cables, observe the following part numbering conventions when ordering a standard 20-foot cable or a specified length of cable. The number 20 followed by the part number denotes the standard 20-foot cable. The letter "L" denotes the specified length required in feet or meters. For example: 9372095-3 denotes a 3 foot cable; 9372095-3M denotes a 3 meter cable.

T1 Specifications

This section provides the Cabletron Systems part number and connector specifications for T1 interface cables.

Table A-1 provides connector type and part number information.

Table A-1 T-1 Interface Cable Part Numbers

Connector Type	Part Number
RJ48C	9372094

Table A-2 provides RJ48 connector pin assignments.

Table A-2 T-1 Connector Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Shield Ground
8	Shield Ground

Table A-3 provides RJ48 DTE pin assignments.

Table A-3 DTE Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Shield Ground
8	Shield Ground

Table A-4 provides RJ48 network pin assignments.

Table A-4 Network Pin Assignments

Pin	Signal
1	Receive Ring
2	Receive Tip
3	Not Used
4	Transmit Ring
5	Transmit Tip
6	Not Used
7	Not Used
8	Not Used

B Specifications and Standards Compliance

This chapter contains hardware specifications, and safety and compliance standards for the HSIM-W84.

Table B-1 Hardware Specifications

WAN Interface	4 T1 ports
Processor	Intel i960 66 Mhz
Power Supply	+5V Supplied by host device
Power Consumption	30 Watts maximum
Operating Temperature	5° to 40°C (41° to 104°F)
Storage Temperature	-30° to 73°C (-22° to 164°F)
Operating Humidity	5% to 90% RH, non-condensing

Regulatory Compliance

Safety — This unit meets the safety requirements of UL 1950, CSA C22.2 No. 950 and EN 60950, IEC 950, and 73/23/EEC.

Electromagnetic Compatibility (EMC) — This unit meets the EMC requirements of FCC Part 15, EN 55022, EN 50082-1, 89/336/EEC, AS/NZS 3548, CSA C108.8, and VCCI V-3.

TELECOM — This unit meets the safety requirements of FCC Part 68, CS-03.

C FCC Part 68 - User's Information For HSIM-W84

The following instructions are to ensure compliance with the Federal Communications Commission (FCC) Rules, Part 68:

1. All connections to the HSIM-W84 must be made using standard plugs and jacks.
2. Before connecting your unit, you must inform the local telephone company of the following information:

Table C-1 HSIM-W84

Port ID	REN/SOC	FIC	USOC
HSIM-W84	6.0N	04DU9-BN 04DU9-DN 04DU9-1KN 04DU9-1SN 04DU9-1ZN	RJ48C RJ48X

3. If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.
4. The CSU/DSU has been designed to prevent harm to the T1 network. If the telephone company finds that the equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give advance notice if possible.
5. Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.
6. If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.
7. The attached Affidavit on the following page must be completed by the installer.
8. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of the users requiring service to report the need for service to our Company or to one of our authorized agents. Refer to the **Getting Help** section of **Chapter 1** for more information on how to get service and support.

AFFIDAVIT FOR THE CONNECTION OF CUSTOMER EQUIPMENT TO 1.544 MBPS AND/OR SUBRATE DIGITAL SERVICES

For the work to be performed in the certified territory of

Telco's name:________________________________

State of:________________________________

Country of:________________________________

I, ______________________________ , of ____

(Name of Authorized Representative) (Customer Name)

_____________________________________ , _____________________________________

(Customer's Address) (Telephone Number)

being duly sworn, state:

I have responsibility for the operation and maintenance of the terminal equipment to be connected to __________________ 1.544 Mbps and/or __________________ Subrate digital services. The terminal equipment to be connected complies with Part 68 of the Commission's rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

- I attest that all operations associated with the establishment, maintenance and adjustment of the digital CPE with respect to encoded analog content and encoded billing information continuously complies with Part 68 of the FCC's Rules and Regulations.
- The digital CPE does not transmit digital signals containing encoded analog or billing information which is intended to be decoded within the telecommunications network.
- The encoded analog and billing protection is factory set and is not under the control of the customer.

I attest that the operator(s) maintainer(s) of the digital CPE responsible for the establishment, maintenance and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully completing one of the following: Check appropriate one(s).

a. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or

b. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or

c. An independent training course (e.g. trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or

d. In lieu of the proceeding training requirements, the operator(s) maintainer(s) is (are) under the control of a supervisor trained in accordance with _________________above.

I agree to provide________________________with proper documentation

(Telco's Name)

to demonstrate compliance with the information as provided in the proceeding paragraph, if so requested.

____ (Signature)

____ (Title)

____ (Date)

Subscribed and sworn to me this ___________ day of ________ , 19____ .

(Notary Public)

My commission expires:

D Glossary

10BASE-T — IEEE 802.3 standard for the use of Ethernet LAN technology over Unshielded Twisted Pair wiring, running at 10 Mbps.

ARP — Address Resolution Protocol. An Internet protocol used to bind an IP address to Ethernet/ 802.3 addresses.

ASCII — American Standard Code for Information Interchange. It is an 8-bit code for character representation.

AUI — Attachment Unit Interface. An IEEE 802.3 transceiver cable connecting the network device (such as a router) to the MAU (media access unit).

Bandwidth on Demand — Feature providing the capability of adjusting the bandwidth (opening or closing multiple B channels) when the load in traffic increases or decreases.

Bridge — A device that segments network traffic. A bridge maintains a list of each node on the segment and only traffic destined for a node on the adjacent segment is passed across the bridge. A bridge operates at Layer 2 of the OSI reference model.

CHAP — Challenge Handshake Authentication Protocol. A security protocol supported under point-to-point protocol (PPP) used to prevent unauthorized access to devices and remote networks. Uses encryption of password, device names and random number generation.

DCE — Data Communicating Equipment. Equipment used within a network to transfer data from source to destination such as modems.

Data Compression — Techniques used to reduce the number of bits transferred across the communication links that represent the actual data bits. Compression is used to optimize use of WAN links and speed data transmission.

DHCP — Dynamic Host Configuration Protocol is a protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

Dial on Demand — Dial up WAN resources are accessed only when remote access is required and released as soon as the resource is no longer needed.

DTE — Data Terminal Equipment. DTE refers to equipment used in a network as the data source and/or destination, such as computers.

DTMF — Dual Tone Multi-Frequency. TOUCHTONE as opposed to Dial Pulse (DP).

DTR — Data Terminal Ready. RS-232 signal used for indicating to the DCE the readiness to transmit and receive data.

EtherTalk — AppleTalk protocols running on Ethernet.

Filter — Feature to control the flow of data based on protocol or bridge information. Filters can be specific to allow data through or prevent transmission.

Firewall — A combination of techniques used to protect one network from unknown networks and users on the outside. Firewalls can filter or block traffic and act as a management and network security point where all traffic can be scrutinized.

Frame — A group of data generated by Data Link Layer operation.

IMUX (Inverse Multiplexing) — The process of splitting a single high-speed channel into multiple signals, transmitting the multiple signals over multiple facilities operating at a lower rate than the original signal, and then recombining the separately-transmitted portions into the original signal at the original rate.

In-Band Signaling — Transmission within the frequency range used for data transmission; i.e., results in use of bandwidth normally reserved for data.

IP — Internet Protocol. A network layer protocol which allows a packet to traverse multiple networks on the way to its final destination.

IP Address — Internet address. A 32-bit address assigned to devices that participate in a network using TCP/IP. An IP address consists of four octets separated with periods defining network, optional subnet and host sections.

IPX (Internet Packet Exchange) — A proprietary Network layer protocol developed by Novell and used in NetWare networks.

Leased Line — A telecommunications line between two service points leased from a communications carrier for private use, usually incurring a monthly service rate.

LEDs (Light Emitting Diodes) — Type of indicator lights on the panel of the router.

Local Area Network (LAN) — A network connecting computers over a relatively small geographic area (usually within a single campus or building).

MAC Layer/Address — Media Access Control layer/address defined by the IEEE 802.3 specification which defines media access including framing and error detection. Part of the OSI reference model Data Link layer.

Metric — An algorithm used by routers to determine the best path for transmitting packets to a remote destination based on considerations such as time, delay, cost, etc.

Modem — Modulator/Demodulator. A device that converts digital signals to/from analog signals for transmission over analog communications lines.

Multi-Link Protocol — A protocol, defined in RFC 1717, that defines a way to perform inverse multiplexing on the TCP/IP point-to-point protocol (PPP); i.e., the ability to use multiple serial WAN channels for transferring one datastream. With MLP, a user can send and receive data over both B channels in an ISDN basic-rate interface connection.

NAT — Network Address Translation uses a unique IP address for a WAN interface. This IP address is negotiated through PPP or assigned statically by the Internet Service Provider (ISP). NAT reduces the number of unique IP addresses for all clients, using a particular WAN interface, to one.

NetWare — A Network Operating System developed by Novell, Inc. providing shared access to files and other network services.

Network Layer — Layer 3 of the OSI reference model that provides the protocol routing function.

Node — Refers to a termination point for communication links; entity that can access a network.

OSI — Open System Interconnection. An international standard developed by ITU (formally CCITT) and ISO (International Organization for Standardization) to facilitate data networking multi-vendor interoperability. The OSI Reference Model defines seven layers, each providing specific network functions.

Packet — A group of data that includes a header and usually user data for transmission through a network.

Ping (Packet Internet Groper) — An echo message, available within the TCP/IP protocol suite, sent to a remote node and returned; used to test the accessibility of the remote node.

PPP (Point-to-Point Protocol) — A Data Link layer protocol that provides asynchronous and synchronous connectivity between computer/network nodes. Includes standardization for security and compression negotiation.

RFC — Request for Comment. Documentation describing Internet communications specifications (e.g., Telnet, TFTP). Often these RFCs are used to achieve multi-vendor interoperability during implementation.

RJ11 — Standard 4-wire connectors for telephone lines.

RJ45 — Standard 8-wire connectors for computer networks.

RIP (Routing Information Protocol) — Protocols used in IP and IPX for broadcasting open path information between routers to keep routing tables current.

Routing — A Network layer function that determines the path for transmitting packets through a network from source to destination.

RS 232 — EIA standard specifying the physical layer interface used to connect a device to communications media.

Serialization Frames — Frames sent out by servers under IPX to check whether illegal copies of NetWare are in use on the network.

Service Advertising Protocol (SAP) — Protocol used by IPX for broadcasting information about services available on the network, such as file servers, CD-ROM drives and modem pools.

SNAP — Sub-Network Access Protocol. An Ethernet or Token Ring frame type that adds additional information to a data packet to allow for identification of the upper layer protocol the packet is destined for.

SNMP — Simple Network Management Protocol. A widely implemented Internet network management protocol that allows status monitoring, getting/setting of parameters for configuration and control of network devices, such as routers and bridges.

Spoofing — Spoofing is a technique used to remove poll and update service frames from WAN links while ensuring that the network continues to operate normally. Spoofing is employed to minimize dial-up line connection time.

Subnet Address — An extension of the Internet 32-bit addressing scheme that allows the separation of physical or logical networks within the single network number assigned to an organization. TCP/IP entities outside this organization have no knowledge of the internal "subnetting."

Subnet Mask — A 32-bit internet protocol address mask used to identify a particular subnetwork.

TCP/IP — Transmission Control Protocol/Internet Protocol. Refers to a set of internetworking protocols developed by the U.S. Department of Defense that define a two level layered approach for interoperability. TCP provides a connection-oriented Transport layer ensuring end-to-end reliability in data transmission. IP provides for Network layer connectivity using connectionless datagrams.

Telco Cloud — The "cloud" of switched virtual connections.

Telnet — Internet standard protocol for remote terminal emulation that allows a user to remotely log in to another device and appear as if directly connected.

TFTP — Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) allowing for file transfer between computers over a network.

Transparent Bridging — Bridging technique used in Ethernet networks that allows transfer of frames across intermediate nodes using tables associating end nodes with bridging addresses. Bridges are unknown to the end nodes.

UDP — User Datagram Protocol. A connectionless protocol used to pass packets across an internet network, requiring no handshaking between source and destination.

Watchdog Frames — Frames sent out by servers to clients, under IPX, to verify that clients are still logged on.

Wide Area Network — A communications network that is geographically dispersed thus requiring links provided by communications carriers.

Workstation — Computer or terminal used by the systems administration or user.

Index